BIPAC 5100S

ADSL Modem/Router
with Single Ethernet Port

User's Manual

Table of Contents

Chapter 1
Getting to Know the BIPAC 5100S

This chapter describes the key features and applications of BIPAC 5100S.

1.1 Introducing the BIPAC 5100S

The BIPAC 5100S integrates high-speed 10/100Mbps auto-negotiating LAN interface and a high-speed ADSL port into a single package. The BIPAC 5100S is ideal for high-speed Internet browsing and making LAN-to-LAN connections to remote networks. By integrating DSL and NAT, the BIPAC 5100S provides super-fast Internet access to multiple users at minimum cost. The BIPAC 5100S is a bridge/router and includes two models, one for ADSL over POTS (Plain Old Telephone System) and one for ADSL over ISDN (Integrated Synchronous Digital System).

The web browser-based Graphical User Interface provides easy management and is totally independent of the operating system platform you use.

1.2 Features of the BIPAC 5100S

The following sections describe the features of the BIPAC 5100S.

➢ **High Speed Internet Access**

The BIPAC 5100S ADSL router can support downstream transmission rates of up to 8 Mbps and upstream transmission rates of 1 Mbps.

➢ **PPPoE Support (RFC2516)**

PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the BIPAC 5100S is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.

➢ **Network Address Translation (NAT)**

Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).

➢ **Universal Plug and Play (UPnP)**

Using the standard TCP/IP protocol, the BIPAC 5100S and other UPnP enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

➢ **10/100M Auto-negotiation Ethernet/Fast Ethernet Interface**

This auto-negotiation feature allows the BIPAC 5100S to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on the Ethernet network.

➢ **Dynamic DNS Support**

With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS client.

➢ **Multiple PVC (Permanent Virtual Circuits) Support**

The BIPAC 5100S supports up to 8 PVC's.

➢ **ADSL Standards**

♦ Full-Rate (ANSI T1.413, Issue 2; G.dmt (G.992.1) with line rate support of up to 8 Mbps downstream and 1 Mbps upstream.

♦ G.lite (G.992.2) with line rate support of up to 1.5Mbps downstream and 512Kbps upstream.

♦ Supports Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.994.1 and G.996.1 (for ISDN only); G.991.1;G.lite (G992.2)).

♦ Supports OAM F4/F5 loop-back, AIS and RDI OAM cells.

♦ ATM Forum UNI 3.1/4.0 PVC.

♦ Supports up to 8 PVCs (UBR, CBR, VBR).

♦ Multiple Protocols over AAL5 (RFC 1483).

♦ PPP over AAL5 (RFC 2364).

♦ PPP over Ethernet (RFC 2516).

➢ **DHCP Support**

DHCP (Dynamic Host Configuration Protocol) allows individual clients (computers) to obtain TCP/IP configuration at start-up from a centralized DHCP server. The BIPAC 5100S has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The BIPAC 5100S can now also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.

➢ **IP Alias**

IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The BIPAC 5100S supports three logical LAN interfaces via its single physical

Ethernet interface with the BIPAC 5100S itself as the gateway for each LAN network.

➢ **IP Policy Routing (IPPR)**

Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.

➢ **Protocol Support**

- ♦ PPP (Point-to-Point Protocol) link layer protocol.
  - PPP over PAP (RFC 1334).
  - PPP over CHAP (RFC 1994).
- ♦ RIP I/RIP II
- ♦ IGMP Proxy
- ♦ ICMP support
- ♦ MIB II support (RFC 1213)
- ♦ PPPoE feature
  - PPPoE idle time out
  - PPPoE dial on demand

➢ **Networking Compatibility**

The BIPAC 5100S is compatible with major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers.

➢ **Multiplexing**

The BIPAC 5100S supports VC-based and LLC-based multiplexing.

➢ **Encapsulation**

The BIPAC 5100S series supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM, MAC encapsulated routing (ENET Encapsulation) as well as PPP over Ethernet (RFC 2516).

➢ **Network Management**

- ♦ Embedded Web Configurator
- ♦ CLI (Command Line Interpreter)
- ♦ SNMP manageable
- ♦ DHCP Server/Client
- ♦ Built-in Diagnostic Tools
- ♦ Syslog
- ♦ TFTP/FTP server, firmware upgrade and configuration backup/support supported

➢ **Diagnostics Capabilities**

- ♦ The BIPAC 5100S can perform self-diagnostic tests. These tests check the integrity of the following circuitry:
  - FLASH memory

- ADSL circuitry
- RAM
- LAN port

➢ **Filters**

The BIPAC 5100S's packet filtering functions allows added network security and management.

➢ **Ease of Installation**

The BIPAC 5100S is designed for quick, intuitive and easy installation.

➢ **Housing**

The BIPAC 5100S's all new compact and ventilated housing minimizes space requirements making it easy to position anywhere in your busy office.

1.3 Applications for the BIPAC 5100S

The BIPAC 5100S is the ideal high-speed Internet access solution. The BIPAC 5100S supports the TCP/IP protocol, which the Internet uses exclusively. It is compatible with all major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers. A DSLAM is a rack of ADSL line cards with data multiplexed into a backbone network interface/connection (for example, T1, OC3, DS3, ATM or Frame Relay).

Chapter 2

Introducing the Web Configurator

This chapter describes how to access and navigate the web configurator.

2.1 Web Configurator Overview

The embedded web configurator allows you to manage the BIPAC 5100S from anywhere through a browser such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. It is recommended that you set your screen resolution to 1024 by 768 pixels

2.2 Accessing the BIPAC 5100S Web Configurator

Step 1. Make sure your BIPAC 5100S hardware is properly connected (refer to the Compact Guide or Read Me First).

Step 2. Prepare your computer/computer network to connect to the BIPAC 5100S (refer to the Compact Guide or Read Me First).

Step 3. Launch your web browser.

Step 4. Type "192.168.1.254" as the URL.

Step 5. An Enter Network Password window displays. Enter the user name ("admin" is the default), password ("admin" is the default) and click OK.

Step 6. You should now see the Site Map screen.

2.3 Navigating the BIPAC 5100S Web Configurator

The following summarizes how to navigate the web configurator from the Site Map screen.
Screens vary slightly for different BIPAC 5100S models.

➢ Click Wizard Setup to begin a series of screens to configure the BIPAC 5100S for the first
time.

➢ Click a link under Advanced Setup to configure advanced BIPAC 5100S features.

➢ Click a link under Maintenance to see BIPAC 5100S performance statistics, upload
firmware and back up, restore or upload a configuration file.

➢ Click SITE MAP to go to the Site Map screen.

➢ Click Logout in the navigation panel when you have finished a BIPAC 5100S
management session.
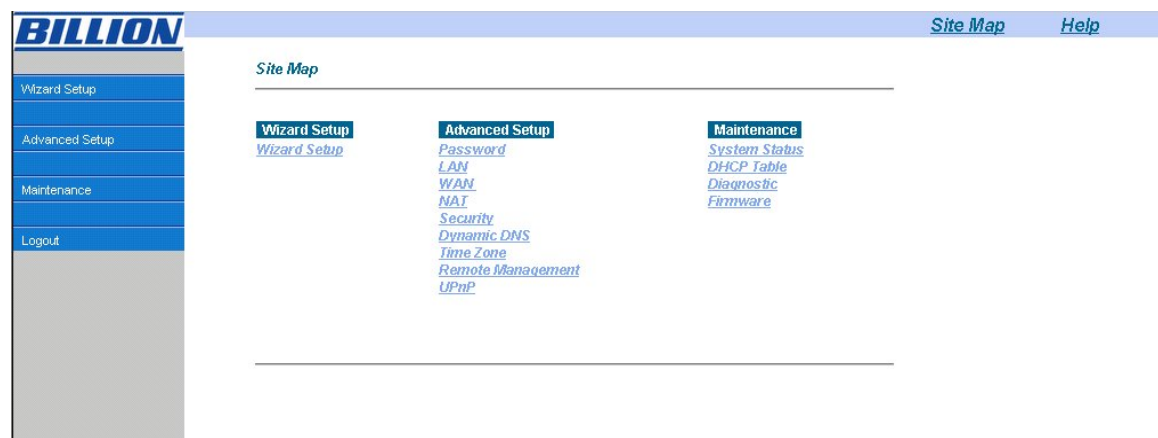
2.4 Configuring Password

It is highly recommended that you change the password for accessing the BIPAC 5100S.
To change the BIPAC 5100S's password, click Advanced Setup and then Password. The
screen appears as shown.

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type the new password in this field.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the BIPAC 5100S.
Cancel	Click **Cancel** to begin configuring this screen afresh.

2.5 Resetting the BIPAC 5100S

If you forget your password or cannot access the BIPAC 5100S, you will need to reload the
factory-default configuration file or use the RESET button the back of the BIPAC 5100S.
Uploading this configuration file replaces the current configuration file with the factory-default
configuration file. This means that you will lose all configurations that you had previously and
the password will be reset to "admin".

2.5.1 Using The Reset Button

Step 1. Make sure the SYS LED is on (not blinking).

Step 2. Press the RESET button for five seconds, and then release it. When the SYS LED
begins to blink, the defaults have been restored and the BIPAC 5100S restarts.

Chapter 3

Wizard Setup

This chapter provides information on the Wizard Setup screens in the web configurator.

3.1 Wizard Setup Introduction

Use the Wizard Setup screens to configure your system for Internet access settings and fill in the fields with the information in the Internet Account Information table of the Compact Guide or Read Me First. Your ISP may have already configured some of the fields in the wizard screens for you.

3.2 Encapsulation

Be sure to use the encapsulation method required by your ISP. The BIPAC 5100S supports the following methods.

3.2.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the Ethernet Encapsulation Gateway field in the second wizard screen. You can get this information from your ISP.

3.2.2 PPP over Ethernet

PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP. The BIPAC 5100S bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to ADSL Access Concentrator where the PPP session terminates. One PVC can support any number of PPP sessions from your LAN. For more information on PPPoE, see the appendix.

3.2.3 PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functionality in a manner similar to dial-up services using PPP. The

BIPAC 5100S encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

3.2.4 RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to the RFC for more detailed information.

3.3 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

3.3.1 VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

3.3.2 LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

3.4 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

3.5 Wizard Setup Configuration: First Screen

In the SITE MAP screen click Wizard Setup to display the first wizard screen.

Wizard Setup- ISP Parameters for Internet Access

Mode	Bridge ▼
Encapsulation	RFC 1483 ▼
Multiplex	LLC ▼
Virtual Circuit ID	
VPI	0
VCI	32

Next

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Mode	From the **Mode** drop-down list box, select **Routing** (default) if your ISP allows multiple computers to share an Internet account. Otherwise select **Bridge**.
Encapsulation	Select the encapsulation type your ISP uses from the **Encapsulation** drop-down list box. Choices vary depending on what you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.
Multiplex	Select the multiplexing method used by your ISP from the **Multiplex** drop-down list box either VC-based or LLC-based.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to
VPI	Enter the VPI assigned to you. This field may already be configured.
VCI	Enter the VCI assigned to you. This field may already be configured.
Next	Click this button to go to the next wizard screen. The next wizard screen you see depends on what protocol you chose above. Click on the protocol link to see the next wizard screen for that protocol.

3.6 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a

LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the BIPAC 5100S. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.254, for your BIPAC 5100S, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your BIPAC 5100S will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the BIPAC 5100S unless you are instructed to do otherwise.

3.7 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and ENET ENCAP Gateway.

3.7.1 IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the IP Address and ENET ENCAP Gateway fields are not applicable (N/A). If you have a static IP, then you only need to fill in the IP Address field and not the ENET ENCAP Gateway field.

3.7.2 IP Assignment with RFC 1483 Encapsulation

In this case the IP Address Assignment must be static with the same requirements for the IP Address and ENET ENCAP Gateway fields as stated above.

3.7.3 IP Assignment with ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the IP Address and ENET ENCAP Gateway fields as supplied by your ISP. However for a dynamic IP,

the BIPAC 5100S acts as a DHCP client on the WAN port and so the IP Address and ENET ENCAP Gateway fields are not applicable (N/A) as the DHCP server assigns them to the BIPAC 5100S.

3.7.4 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

3.8 Nailed-Up Connection (PPP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The BIPAC 5100S does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the BIPAC 5100S will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern

3.9 NAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

3.10 Wizard Setup Configuration: Second Screen

The second wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click Next to continue.

3.10.1 PPPoE

Select PPPoE from the Encapsulation drop-down list box in the first wizard screen to display the screen as shown.

Wizard Setup- ISP Parameters for Internet Access

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Service Name	Type the name of your PPPoE service here.
User Name	Configure **User Name** and **Password** fields for **PPPoA** and **PPPoE** encapsulation only. Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address. Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** text box below.
Connection	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out (in seconds) in the **Max. Idle Timeout** field. The default setting selects **Connection on Demand** with 0 as the idle time-out, which means the Internet session will Select **Nailed-Up Connection** when you want your connection up all the time. The BIPAC 5100S will try to bring up the connection automatically if it is disconnected.

Network Address Translation	Select **None**, **SUA Only** or **Full Feature** from the drop-sown list box. Refer to the NAT chapter for more details.
Back	Click **Back** to go back to the first wizard screen.
Next	Click **Next** to continue to the next wizard screen.

3.10.2 RFC 1483

Select RFC 1483 from the Encapsulation drop-down list box in the first wizard screen to display the screen as shown.

Wizard Setup- ISP Parameters for Internet Access

IP Address   0.0.0.0

Network Address Translation
     SUA Only

Back   Next

The following table describes the labels in this screen.

LABEL	DESCRIPTION
IP Address	This field is available if you select **Routing** in the **Mode** field. Type your ISP assigned IP address in this field.
Network Address Translation	Select **None**, **SUA Only** or **Full Feature** from the drop-sown list box. Refer to the NAT chapter for more details.
Network Address Translation	Select **None**, **SUA Only** or **Full Feature** from the drop-sown list box. Refer to the NAT chapter for more details.
LABEL	DESCRIPTION
Back	Click **Back** to go back to the first wizard screen.
Next	Click **Next** to continue to the next wizard screen.

3.10.3 ENET ENCAP

Select ENET ENCAP from the Encapsulation drop-down list box in the first wizard screen to display the screen as shown.

Wizard Setup- ISP Parameters for Internet Access

IP Address

    ○   Obtain an IP Address Automatically

    ○   Static IP Address

             IP Address   0.0.0.0

             Subnet Mask   0.0.0.0

             Gateway   0.0.0.0

Network Address Translation

          SUA Only ▾

Back   Next

The following table describes the labels in this screen.

LABEL	DESCRIPTION
IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address. Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** text box below.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the *IP Subnetting* appendix to calculate a subnet mask If you are implementing subnetting.
ENET ENCAP Gateway	You must specify a gateway IP address (supplied by your ISP) when you use **ENET ENCAP** in the **Encapsulation** field in the previous screen.
Network Address Translation	Select **None**, **SUA Only** or **Full Feature** from the drop-sown list box. Refer to the NAT chapter for more details.
Back	Click **Back** to go back to the first wizard screen.
Next	Click **Next** to continue to the next wizard screen.

3.10.4 PPPoA

Select PPPoA from the Encapsulation drop-down list box in the first wizard screen to display the screen as shown.

19

Wizard Setup- ISP Parameters for Internet Access

User Name [ ]

Password [ ]

IP Address

- ⦿ Obtain an IP Address Automatically
- ◯ Static IP Address
  [0.0.0.0]

Connection

- ◯ Connect on Demand: Max Idle Timeout [0] sec
- ⦿ Nailed-Up Connection

Network Address Translation
[SUA Only ▼]

Back   Next

The following table describes the labels in this screen.

LABEL	DESCRIPTION
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
IP Address	This option is available if you select **Routing** in the **Mode** field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address. Click **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise click **Static IP Address** and type your ISP assigned IP address in the **IP Address** text box below
Connection	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out (in seconds) in the **Max. Idle Timeout** field. The default setting selects **Connection on Demand** with 0 as the idle time-out, which means the Internet session will not timeout Select **Nailed-Up Connection** when you want your connection up all the time. The BIPAC 5100S will try to bring up the connection automatically if it is disconnected.
Network Address	This option is available if you select **Routing** in the **Mode** field.

Translation	Select **None**, **SUA Only** or **Full Feature** from the drop-sown list box. Refer to the NAT chapter for more details.
Back	Click **Back** to go back to the first wizard screen.
Next	Click **Next** to continue to the next wizard screen.

3.11 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the BIPAC 5100S as a DHCP server or disable it. When configured as a server, the BIPAC 5100S provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

3.11.1 IP Pool Setup
The BIPAC 5100S is pre-configured with a pool of 100 IP addresses starting from 192.168.1.100 to 192.168.1.199 for the client machines.

3.12 Wizard Setup Configuration: Third Screen

Verify the settings in the screen shown next. To change the LAN information on the BIPAC 5100S, click Change LAN Configurations. Otherwise click Save Settings to save the configuration and skip to section 3.13.

Wizard Setup- ISP Parameters for Internet Access

WAN Information:
Mode: **Routing**
Encapsulation: **PPPoE**
Multiplexing: **LLC**
VPI/VCI: **0/32**
Service Name:
User Name: **username**
Password: ********
IP Address: **Obtain an IP Address Automatically**
Network Address Translation: **SUA Only**
Connection: **Nailed-Up Connection**

LAN Information:
IP Address: **192.168.1.254**
IP Mask: **255.255.255.0**
DHCP: **ON**
Client IP Pool Starting Address: **192.168.1.100**
Size of Client IP Pool: **100**

Change LAN Configuration

Save Settings

If you want to change your BIPAC 5100S LAN settings, click Change LAN Configuration to display the screen as shown next.

Wizard Setup- ISP Parameters for Internet Access

LAN IP Address	192.168.1.254
LAN Subnet Mask	255.255.255.0

DHCP

DHCP Server	ON
Client IP Pool Starting Address	192.168.1.100
Size of Client IP Pool	100
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

Back   Finish

The following table describes the labels in this screen.

LABEL	DESCRIPTION
LAN IP Address	Enter the IP address of your BIPAC 5100S in dotted decimal notation, for example, 192.168.1.254 (factory default).
LAN Subnet Mask	Enter a subnet mask in dotted decimal notation.
DHCP	
DHCP Server	From the **DHCP Server** drop-down list box, select **On** to allow your BIPAC 5100S to assign IP addresses, an IP default gateway and DNS servers to computer systems that support the DHCP client. Select **Off** to disable DHCP server. When DHCP server is used, set the following items:
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Back	Click **Back** to go back to the first wizard screen.
Finish	Click **Finish** to save the settings and proceed to the next wizard screen.

3.13 Wizard Setup Configuration: Connection Tests

The BIPAC 5100S automatically tests the connection to the computer(s) connected to the LAN ports. To test the connection from the BIPAC 5100S to the ISP, click Start Diagnose. Otherwise click Return to Main Menu to go back to the Site Map screen.

Wizard Setup- ISP Parameters for Internet Access

Your DSL Gateway is now configured. Your device is capable of testing your DSL service. The individual tests are listed below. Click "Start Diagnose" button if you want to test; otherwise, click "Return to Main Menu" button.

LAN connections

Test your Ethernet Connection	**PASS**

WAN connections

Test ADSL synchronization	**N/A**
Test ADSL(ATM OAM) loopback test	**N/A**
Test PPP/PPPoE server connection	**N/A**
Ping default gateway	**N/A**

Start Diagnose   Return to Main Menu

3.14 Test Your Internet Connection

Launch your web browser and navigate to www.billion.com. Internet access is just the beginning. Refer to the rest of this User's Guide for more detailed information on the complete range of BIPAC 5100S features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the Wizard Setup are correct.

Chapter 4
LAN Setup

*This chapter describes how to configure LAN settings.*

4.1 LAN Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building.

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

4.1.1 LANs, WANs and the BIPAC 5100S

The actual physical connection determines whether the BIPAC 5100S ports are LAN or WAN ports. There are two separate IP networks, one inside, the LAN network; the other outside: the WAN network as shown next:
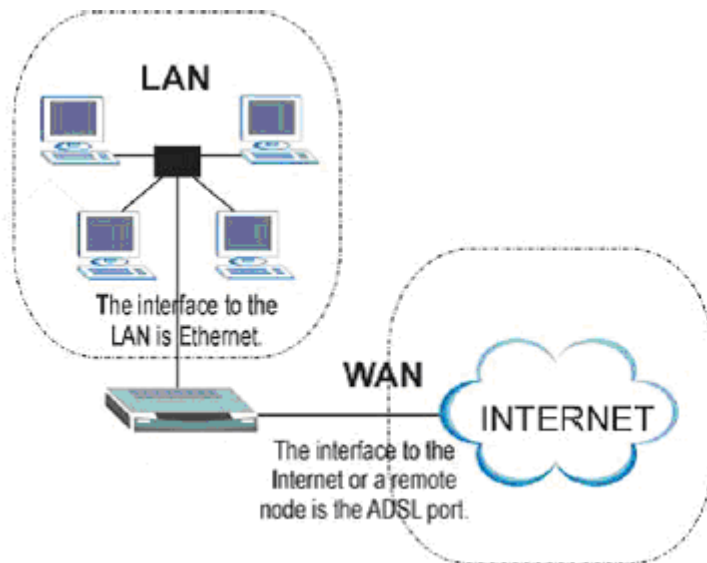
4.2 DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, for example, the IP address of www.billion.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup are

passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP gives you the DNS server addresses, enter them in the DNS Server fields in DHCP Setup, otherwise, leave them blank.

Some ISP's choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The BIPAC 5100S supports the IPCP DNS server extensions through the DNS proxy feature.

If the Primary and Secondary DNS Server fields in DHCP Setup are not specified, for instance, left as 0.0.0.0, the BIPAC 5100S tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the BIPAC 5100S, the BIPAC 5100S forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the DHCP Setup menu. This way, the BIPAC 5100S can pass the DNS servers to the computers and the computers can query the DNS server directly without the BIPAC 5100S's intervention.

4.3 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

There are two ways that an ISP disseminates the DNS server addresses.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.

2. Leave the DNS Server fields in DHCP Setup blank (for example 0.0.0.0). The BIPAC 5100S acts as a DNS proxy when this field is blank.

4.4 LAN TCP/IP

The BIPAC 5100S has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

4.4.1 Factory LAN Defaults

The LAN parameters of the BIPAC 5100S are preset in the factory with the following values:

 ➢ IP address of 192.168.1.254 with subnet mask of 255.255.255.0 (24 bits)

> DHCP server enabled with 100 client IP addresses starting from 192.168.1.100.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

4.4.2 IP Address and Subnet Mask

Refer to the IP Address and Subnet Mask section in the Wizard Setup chapter for this information.

4.4.3 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction field controls the sending and receiving of RIP packets. When set to:

1. Both - the BIPAC 5100S will broadcast its routing table periodically and incorporate the RIP information that it receives.

2. In Only - the BIPAC 5100S will not send any RIP packets but will accept all RIP packets received.

3. Out Only - the BIPAC 5100S will send out RIP packets but will not accept any RIP packets received.

4. None - the BIPAC 5100S will not send any RIP packets and will ignore any RIP packets received.

The Version field controls the format and the broadcasting method of the RIP packets that the BIPAC 5100S sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting.

4.4.4 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP.

The address 224.0.0.2 is assigned to the multicast routers group.

The BIPAC 5100S supports both IGMP version 1 (IGMP-v1) and IGMP version 2 (IGMP-v2). At start up, the BIPAC 5100S queries all directly connected networks to gather group membership. After that, the BIPAC 5100S periodically updates this information. IP multicasting can be enabled/disabled on the BIPAC 5100S LAN and/or WAN interfaces in the web configurator (LAN; WAN). Select None to disable IP multicasting on these interfaces.

4.5 Configuring LAN

Click LAN to open the following screen.

The following table describes the labels in this screen.

LABEL	DESCRIPTION
DHCP	If set to **Server**, your BIPAC 5100S can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.
	If set to **None**, the DHCP server will be disabled.
	If set to **Relay**, the BIPAC 5100S acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.
	When DHCP is used, the following items need to be set:

LAN Subnet Mask	Enter a subnet mask in dotted decimal notation.
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.
TCP/IP	
IP Address	Enter the IP address of your BIPAC 5100S in dotted decimal notation, for example, 192.168.1.254 (factory default).
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
RIP Direction	Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. The BIPAC 5100S supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Select **None** to disable it.
Apply	Click this button to save these settings back to the BIPAC 5100S.
Cancel	Click this button to reset the fields in this screen.

Chapter 5
WAN Setup

This chapter describes how to configure WAN settings.

5.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet.
See the Wizard Setup chapter for more information on the fields in the WAN screens.

5.2 PPPoE Encapsulation

The BIPAC 5100S supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF
Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a
broadband modem (DSL, cable, wireless, etc.) connection. The PPPoE option is for a dial-up
connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with
existing access control systems (for example Radius). PPPoE provides a login and
authentication method that the existing Microsoft Dial-Up Networking software can activate,
and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a
function known as dynamic service selection. This enables the service provider to easily
create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires
no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the BIPAC 5100S (rather than individual computers), the
computers on the LAN do not need PPPoE software installed, since the BIPAC 5100S does
that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

5.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of
data from a remote client to a private server, creating a Virtual Private Network (VPN) using
TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

5.4 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and "burstiness" or fluctuation of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 1 Mbps gives a maximum PCR of 2415 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

Sustained Cell Rate (SCR) is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. SCR may not be greater than the PCR; the system default is 0 cells/sec.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

The following figure illustrates the relationship between PCR, SCR and MBS.
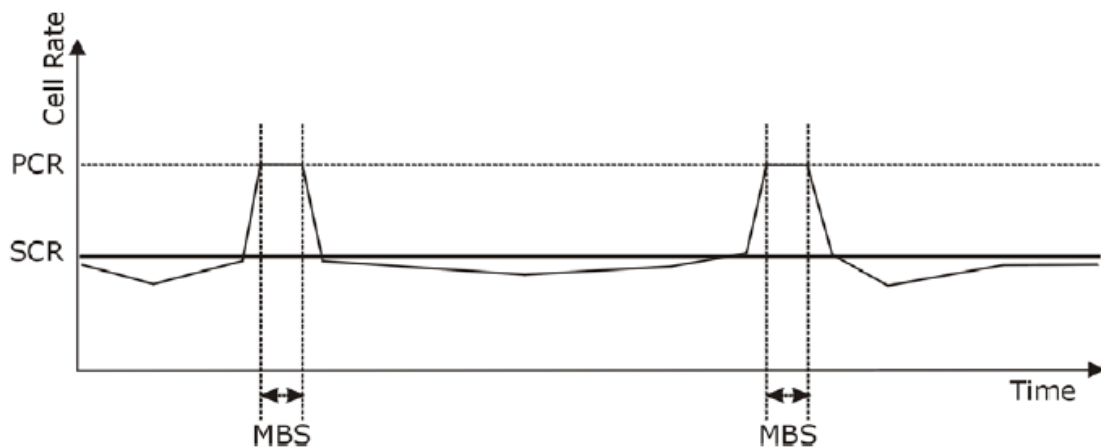
5.5 Configuring WAN Setup

To change your BIPAC 5100S's WAN remote node settings, click WAN. The screen differs by the encapsulation.

Wan - Wan List

☑ Route
☐ Bridge
☐ Half Bridge

	Name	Active	Mode	VPI	VCI	Encap	IP Address
Profile 1	isp	Yes	Bridge	0	32	RFC 1483	-
Profile 2	-	-	-	-	-	-	-
Profile 3	-	-	-	-	-	-	-
Profile 4	-	-	-	-	-	-	-
Profile 5	-	-	-	-	-	-	-
Profile 6	-	-	-	-	-	-	-
Profile 7	-	-	-	-	-	-	-
Profile 8	-	-	-	-	-	-	-

Back   Apply

5.5.1 PPP Half Bridge

When the PPP Half Bridge is enabled the BIPAC 5100S becomes invisible. The DHCP server will duplicate the WAN IP address from the ISP to the local client PC. Only one PC is able to access the Internet using half bridge mode.

Half bridge mode can only be used when a single IP address has been assigned by the ISP, it is not suitable for services that provide multiple IP addresses. Half bridge mode is used when the use of NAT or NAPT is not desired and there is a single computer attached to the BIPAC 5100S ADSL Gateway.

5.5.2 When to use Half Bridge mode

When using a separate firewall that will be protecting the network, half bridge mode will allow the firewall to appear on the internet using the publicly accessible IP address assigned by the ISP. This configuration will allow the dedicated firewall to have full control of the inbound and outbound traffic and is the intended purpose for this mode.

Some applications that embed the IP address of the computer in the data are not compatible with NAT or NAPT and so the computer requires a real public IP address. However the number of applications that are not compatible with NAT/NAPT are reducing as developers address the issues. Before deciding to use half bridge mode please check to see if the application can be made to work using the virtual server port forwarding feature on the BIPAC 5100S. Using NAT/NAPT is preferable as it provides the first line of defence against attack from hackers/crackers and allows the connection of more than one computer.

WAN - WAN Setup - Profile 1

Name	isp
Active	Yes ▼

Mode	Routing ▼
Encapsulation	PPPoE ▼
Multiplex	LLC ▼
Virtual Circuit ID	
VPI	0
VCI	32
ATM QoS Type	UBR ▼
Cell Rate	
Peak Cell Rate	0 cell/sec
Sustain Cell Rate	0 cell/sec
Maximum Burst Size	0
Login Information	
Service Name	
User Name	
Password	*

IP Address

○ Obtain an IP Address Automatically

◉ Static IP Address

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0

Connection

◉ Connect on Demand: Max Idle Timeout 0 sec

○ Nailed-Up Connection

TCP MSS Option

TCP MSS(0 means use default) 0 bytes

Back   Apply   Reset

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Name	Enter the name of your Internet Service Provider, e.g., MyISP. This information is for identification purposes only.
Mode	Select **Routing** (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select **Bridge**.

Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.
Multiplex	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
ATM QoS Type	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications. **VBR** is not available on all models.
Cell Rate	Cell rate configuration often helps eliminate traffic congestion that slows transmission of real time data such as audio and video connections.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Login Information	(PPPoA and PPPoE encapsulation only)
Service Name	(PPPoE only) Type the name of your PPPoE service here.
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address. Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** field below.
Connection	The schedule rule(s) have priority over your **Connection** settings.

(PPPoA and PPPoE encapsulation only)	
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The BIPAC 5100S will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
Subnet Mask (ENET ENCAP encapsulation only)	Enter a subnet mask in dotted decimal notation. Refer to the *Subnetting* appendix in the to calculate a subnet mask If you are implementing subnetting.
ENET ENCAP Gateway (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select **ENET ENCAP** in the **Encapsulation** field.
TCP MSS Option (PPPoA/PPPoE, Routing mode only)	This will increase the current MSS limit to the number specified, hence the tweak test will report Max Packet Size as the specified number plus 40*. The catch is that every time your PPPoE disconnects and re-connects it will revert back to MSS limit of 1400 (Max packet size of 1440) and needs to be entered after PPPoE connects again. This function does not work before PPPoE connects. *Referring to RFC879, the MSS value = MTU - 40, so by limiting the MSS value, you will get limited MTU value.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 6

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the BIPAC 5100S*.*

6.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

6.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the BIPAC 5100S, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

| ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

6.1.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination

address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. With no servers defined, your BIPAC 5100S filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to RFC 1631, The IP Network Address Translator (NAT).

6.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The BIPAC 5100S keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.
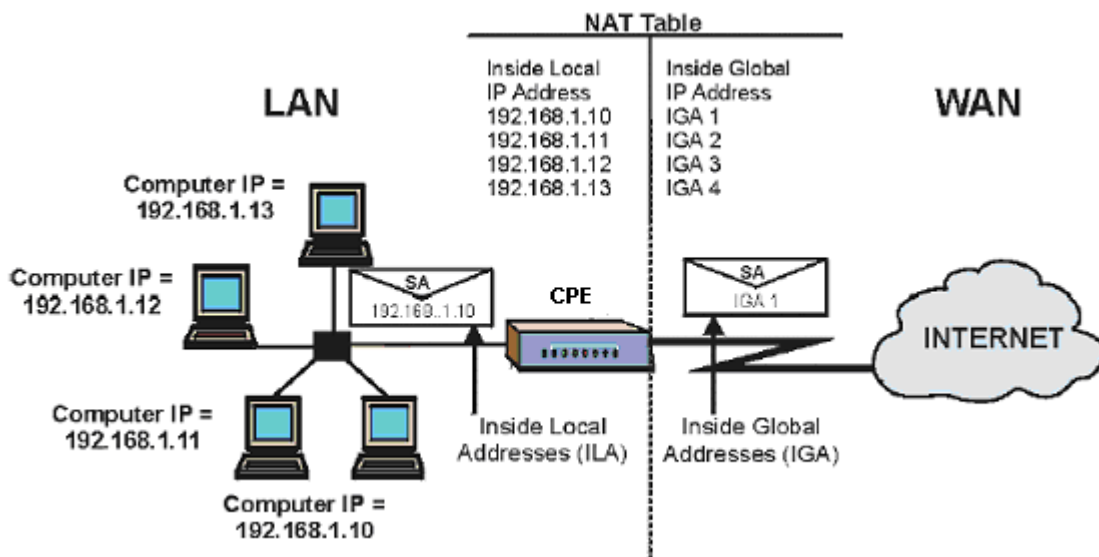
6.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the BIPAC 5100S can communicate with three distinct WAN networks. More examples follow at the end of this chapter.
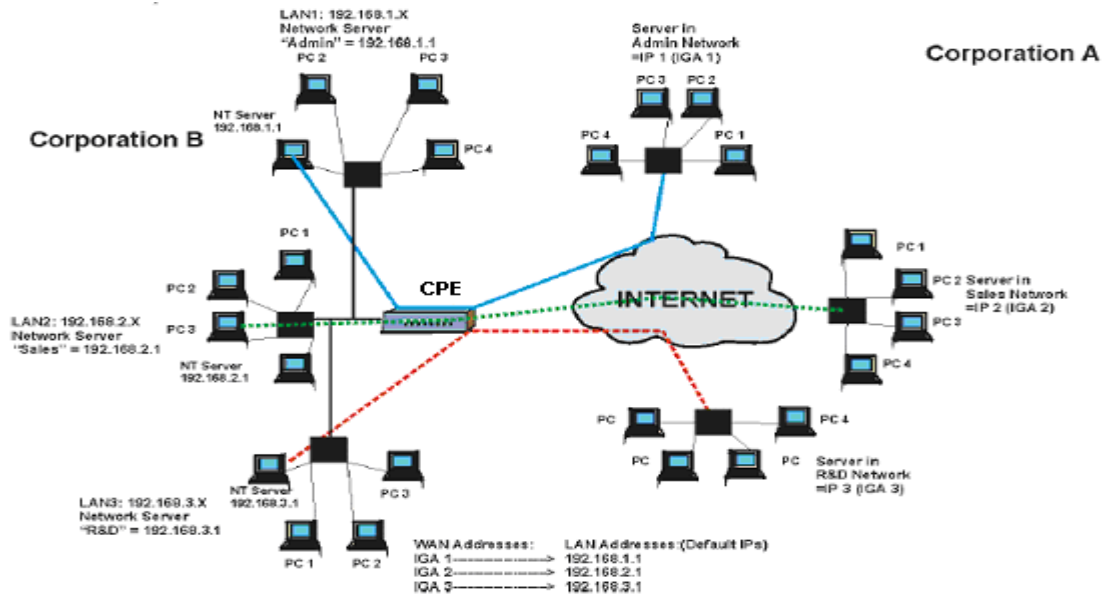
6.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

1. One to One: In One-to-One mode, the BIPAC 5100S maps one local IP address to one global IP address.

2. Many to One: In Many-to-One mode, the BIPAC 5100S maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), Billion's Single User Account feature that previous Billion routers supported (the SUA Only option in today's routers).

3. Many to Many Overload: In Many-to-Many Overload mode, the BIPAC 5100S maps the multiple local IP addresses to shared global IP addresses.

4. Many-to-Many No Overload: In Many-to-Many No Overload mode, the BIPAC 5100S maps each local IP address to a unique global IP address.

5. Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

The following table summarizes these types.

TYPE	IP MAPPING	
One-to-One	ILA1	IGA1
Many-to-One (SUA/PAT)	ILA1	IGA1
	ILA2	IGA1
	…	
Many-to-Many Overload	ILA1	IGA1
	ILA2	IGA2
	ILA3	IGA1
	ILA4	IGA2
	. . .	

Many-to-Many No Overload	ILA1 IGA1
	ILA2 IGA2
	ILA3 IGA3
	…
Server	Server 1 IP IGA1
	Server 2 IP IGA1
	Server 3 IP IGA1

6.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a implementation of a subset of NAT that supports two types of mapping, Many-to-One and Server. The BIPAC 5100S also supports Full Feature NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in

6.3 SUA Server

A SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

6.3.1 Port Forwarding: Services and Port Numbers

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use the SUA Server page to forward incoming service requests to the server(s) on your local

network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers.

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

6.3.2 Configuring Servers Behind SUA (Example)

Let's say you want to assign ports 22-25 to one server, port 80 to another and assign a default server IP address of 192.168.1.35 as shown in the next figure.
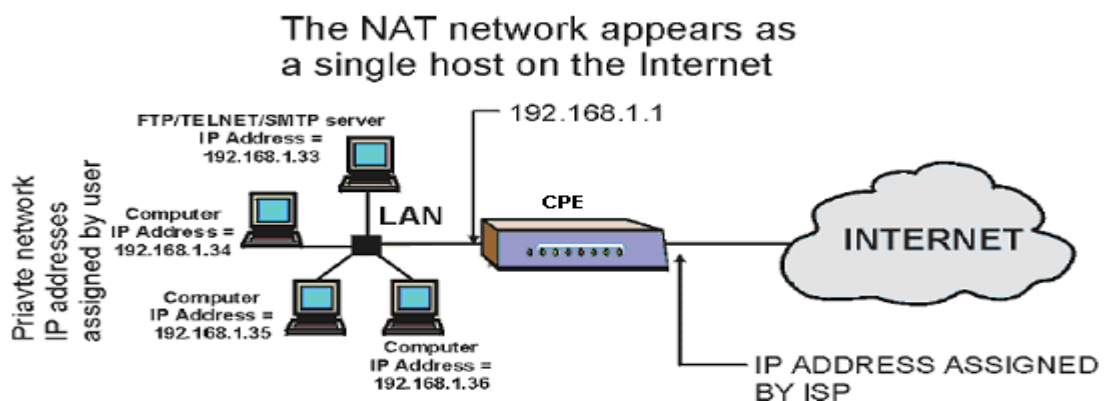
6.4 Selecting the NAT Mode

Click NAT to open the following screen.

The following table describes the labels in this screen.

LABEL	DESCRIPTION
None	Select this radio button to disable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your BIPAC 5100S. The BIPAC 5100S uses Address Mapping Set 1 in the **NAT - Edit SUA/NAT Server Set** screen.
Edit Details	Click this link to go to the **NAT - Edit SUA/NAT Server Set** screen.
Full Feature	Select this radio button if you have multiple public WAN IP addresses for your BIPAC 5100S.
Edit Details	Click this link to go to the **NAT - Address Mapping Rules** screen.
Apply	Click **Apply** to save your configuration.

6.5 Configuring SUA Server

Click NAT, Select SUA Only and click Edit Details to open the following screen.

NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	0	0	0.0.0.0
3	0	0	0.0.0.0
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	0	0	0.0.0.0

Save   Reset

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Start Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the **End Port No.** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port No.** field.
End Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the **Start Port No.** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port No.** field above.
IP Address	Enter your server IP address in this field.
Save	Click **Save** to save your changes back to the BIPAC 5100S.
Cancel	Click **Cancel** to return to the previous configuration.

6.6 Configuring Address Mapping

Ordering your rules is important because the BIPAC 5100S applies the rules in the order that

you specify. When a rule matches the current packet, the BIPAC 5100S takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your BIPAC 5100S's address mapping settings, click NAT, Select Full Feature and click Edit Details to open the following screen.

NAT - Address Mapping Rules

	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
Rule 1	. . .	. . .	. . .	. . .	-
Rule 2	. . .	. . .	. . .	. . .	-
Rule 3	. . .	. . .	. . .	. . .	-
Rule 4	. . .	. . .	. . .	. . .	-
Rule 5	. . .	. . .	. . .	. . .	-
Rule 6	. . .	. . .	. . .	. . .	-
Rule 7	. . .	. . .	. . .	. . .	-
Rule 8	. . .	. . .	. . .	. . .	-
Rule 9	. . .	. . .	. . .	. . .	-
Rule 10	. . .	. . .	. . .	. . .	-

Back

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-one** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-one**, **Many-to-One** and **Server** mapping types.
Type	**1-1**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **M-1**: Many-to-One mode maps multiple local IP addresses to one global IP address.

	This is equivalent to SUA (i.e., PAT, port address translation), Billion's Single User Account feature that previous Billion routers supported only.
	M-M Ov (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.
	MM No (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.
	Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Back	Click **Back** to return to the **NAT Mode** screen.

6.7 Editing an Address Mapping Rule

To edit an address mapping rule, click the rule's link in the NAT Address Mapping Rules screen to display the screen shown next.

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following.
	1. **One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type.
	2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), Billion's Single User Account feature that previous Billion routers supported only.
	3. **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.
	4. **Many-to-Many No Overload**: Many-to-Many No Overload mode maps each

	local IP address to unique global IP addresses.
	5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-one** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-one**, **Many-to-One** and **Server** mapping types.
Server Mapping Set	Only available when **Type** is set to **Server**. Select a number from 1 to 10 from the drop-down menu to choose a server set from the **NAT - Address Mapping Rules** screen.
Edit Details	Click this link to go to the **NAT - Edit SUA/NAT Server Set** screen to edit a server set that you have selected in the **Server Mapping Set** field.
Apply	Click **Apply** to save your changes back to the BIPAC 5100S.
Cancel	Click **Cancel** to return to the previously saved settings.
Delete	Click **Delete** to exit this screen without saving

Chapter 7

Dynamic DNS Setup

This chapter discusses how to configure your BIPAC 5100S to use Dynamic DNS.

7.1 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a DNS-like address (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a DNS name. The Dynamic DNS service provider will give you a password or key.

7.1.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

7.2 Configuring Dynamic DNS

To change your BIPAC 5100S's DDNS, click Dynamic DNS. The screen appears as shown.

Dynamic DNS

☐ Active

Service Provider   WWW.DynDNS.ORG ▾

Host Name

E-mail Address

User

Password

☐ Enable Wildcard

Apply   Reset

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Active	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your BIPAC 5100S by your Dynamic DNS provider.
E-mail Address	Type your e-mail address.
User	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard	Select this check box to enable DYNDNS Wildcard.
Apply	Click **Apply** to save your changes back to the BIPAC 5100S.
Cancel	Click **Cancel** to return to the previously saved settings.

Chapter 8

Time and Date Setup

Use this screen to configure the BIPAC 5100S's time and date settings. This chapter is not available on all models.

8.1 Configuring Time Zone

To change your BIPAC 5100S's time and date, click Time Zone. The screen appears as shown. Use this screen to configure the BIPAC 5100S's time based on your local time zone.

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Time Server	
Use Time Server when Bootup	Select the time service protocol that your time server sends when you turn on the BIPAC 5100S. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server.

	Time (RFC 868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305),** is similar to Time (RFC 868). Select **None** to enter the time and date manually.
Time Server IP Address	Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected **Daylight Savings**.
End Date	Enter the month and day that your daylight-savings time ends on if you selected **Daylight Savings**.
Calibrate system clock with Time Server now	Click this button to have your BIPAC 5100S use the time server (that you configured above) to set its internal system clock. Please wait for up to 60 seconds while the BIPAC 5100S locates the time server. If the BIPAC 5100S cannot find the time server, please check the time server protocol and its IP address. If the IP address was entered correctly, try pinging it for example to test the connection.
Date	
Current Date	This field displays the date of your BIPAC 5100S. Each time you reload this page, the BIPAC 5100S synchronizes the time with the time server.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server. When you select **None** in the **Use Time Server when Bootup** field, enter the new date in this field and then click **Apply**.
Time	
Current Time	This field displays the time of your BIPAC 5100S. Each time you reload this page, the BIPAC 5100S synchronizes the time with the time server.
New Time	This field displays the last updated time from the time server. When you select **None** in the **Use Time Server when Bootup** field, enter the new time in this field and then click **Apply**.
Apply	Click **Apply** to save your changes back to the BIPAC 5100S.
Cancel	Click **Cancel** to return to the previously saved settings.

Chapter 9

Remote Management Configuration

This chapter provides information on configuring remote management. Remote management is not available on all models

9.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which BIPAC 5100S interface (if any) from which computers.

You may manage your BIPAC 5100S from a remote location via:

> ➢ Internet (WAN only)   ➢ ALL (LAN and WAN)

> ➢ LAN only   ➢ Neither (Disable)

To disable remote management of a service, select Disable in the corresponding Server Access field.

9.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in one of the remote management screens.
3. The IP address in the Secured Client IP field does not match the client IP address. If it does not
4. There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.
5. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

9.1.2 Remote Management and NAT

When NAT is enabled:

> ➢   Use the BIPAC 5100S's WAN IP address when configuring from the WAN.
> ➢   Use the BIPAC 5100S's LAN IP address when configuring from the LAN.

9.1.3 System Timeout

There is a system timeout of five minutes (three hundred seconds) for telnet/web/FTP connections. Your BIPAC 5100S automatically logs you out if you do nothing in this timeout

period, except when sys stdio has been changed on the command line.

9.2 Telnet

You can configure your BIPAC 5100S for remote Telnet access as shown next.
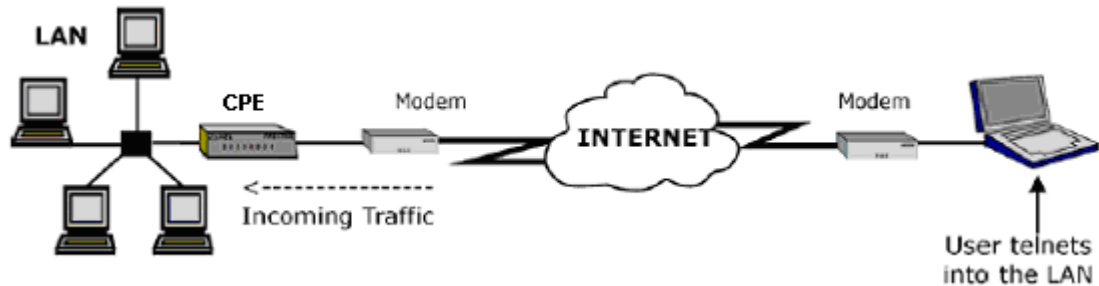
9.3 FTP

You can upload and download BIPAC 5100S firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

9.4 Web

You can use the BIPAC 5100S's embedded web configurator for configuration and file management. See the online help for details.

9.5 Configuring Remote Management

Click Remote Management to open the following screen.

Remote Management Control

Server Type	Access Status	Port	Secured Client IP
Telnet	All	23	0.0.0.0
FTP	All	21	0.0.0.0
Web	All	80	0.0.0.0

Apply   Reset

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Server Type	Each of these labels denotes a service that you may use to remotely manage the BIPAC 5100S.
Access Status	Select the access interface. Choices are **All**, **LAN Only**, **WAN Only** and **Disable**.
Port	This field shows the port number for the remote management service. You may change the port number for a service in this field, but you must use the same port umber to use that service for remote management.
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the BIPAC 5100S. Type an IP address to restrict access to a client with a matching IP address.
Apply	Click **Apply** to save your settings back to the BIPAC 5100S.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 10

Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

10.1 Universal Plug and Play Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. An UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

10.1.1 How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

10.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

> ➢ Dynamic port mapping
>
> ➢ Learning public IP addresses
>
> ➢ Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP. See the *Network Address Translation (NAT)* chapter for further information about NAT.

10.2 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

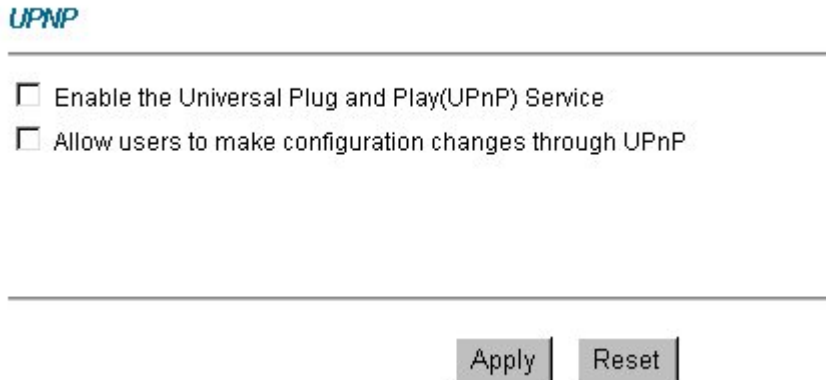All UPnP-enabled devices may communicate freely with each other without additional

configuration. Disable UPnP if this is not your intention.

UPnP broadcasts are only allowed on the LAN.

See later sections for examples of installing UPnP in Windows XP and Windows Me as well as

an example of using UPnP in Windows.

10.2.1 Configuring UPnP

From the Site Map in the main menu, click UPnP under Advanced Setup to display the screen
shown next.

The following table describes the labels in this screen.

| LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Service	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the BIPAC 5100S's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the BIPAC 5100S so that they can communicate through the BIPAC 5100S, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Apply	Click **Apply** to save your settings back to the BIPAC 5100S.
Cancel	Click **Cancel** to return to the previously saved settings.

10.3 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.
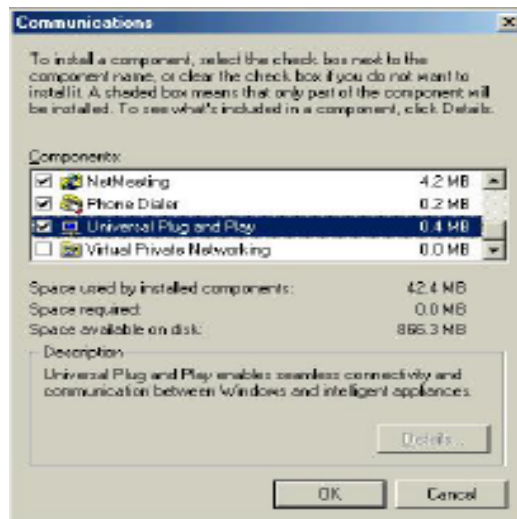
10.3.1 Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

Step 1. Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2. Click on the Windows Setup tab and select Communication in the Components

selection box. Click Details.
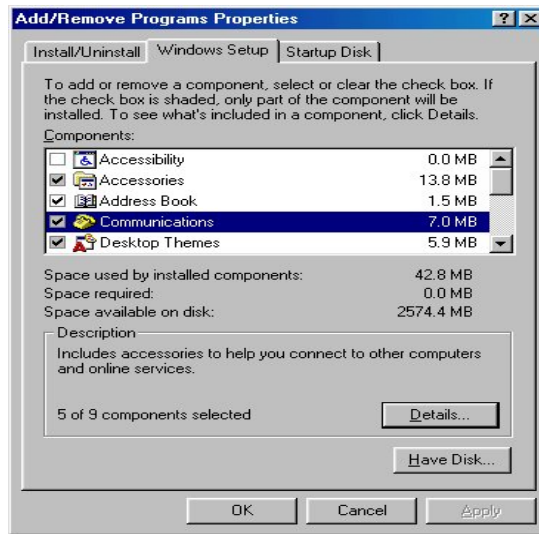
Step 3. In the Communications window, select the Universal Plug and Play check box in the

Components selection box.

Step 4. Click OK to go back to the Add/Remove Programs Properties window and click Next.
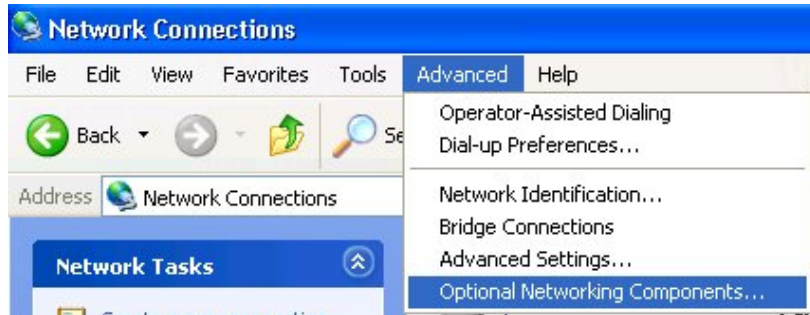
Step 5. Restart the computer when prompted.

10.3.2 Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

Step 1. Click Start and Control Panel.

Step 2. Double-click Network Connections.

Step 3. In the Network Connections window, click Advanced in the main menu and select

Optional Networking Components ….

The Windows Optional Networking Components Wizard window displays.

Step 4. Select Networking Service in the Components selection box and click Details.
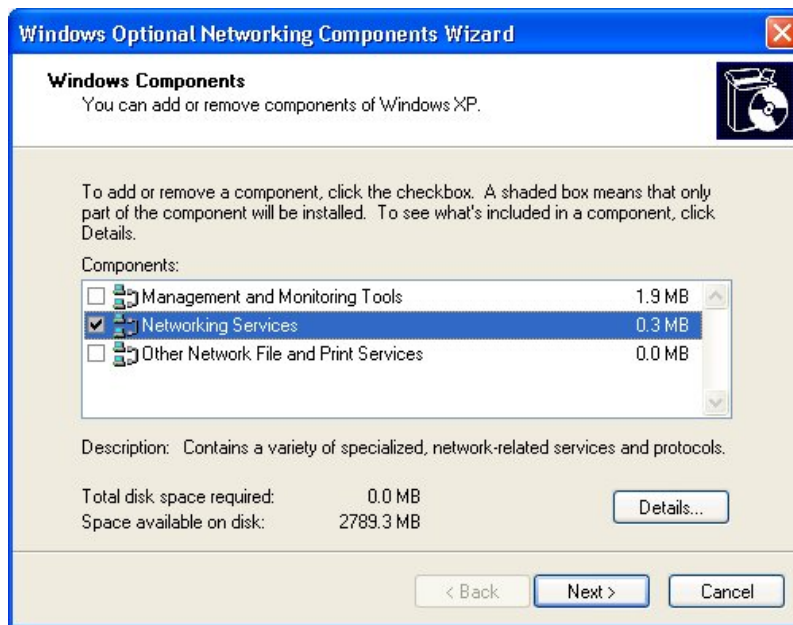
Step 5. In the Networking Services window, select the Universal Plug and Play check box.

Step 6. Click OK to go back to the Windows Optional Networking Component Wizard window and click Next.
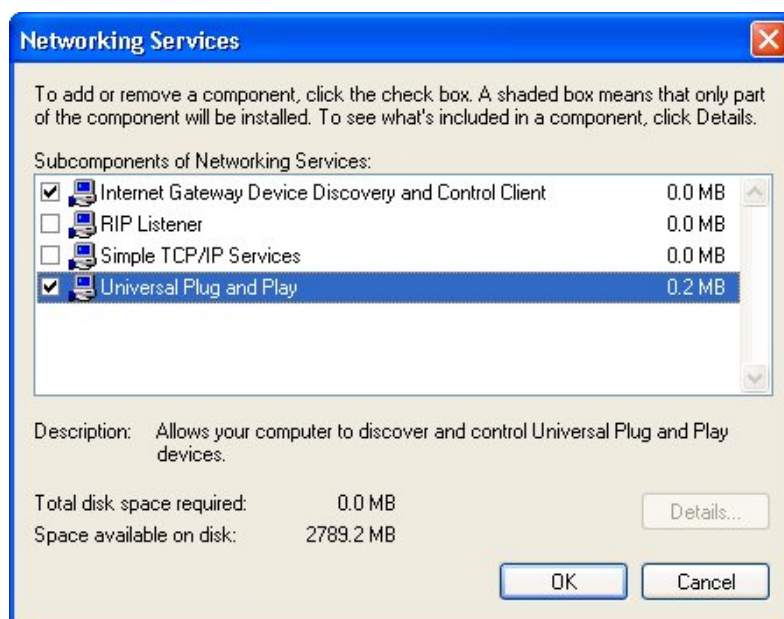
10.4 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the BIPAC 5100S.

Make sure the computer is connected to a LAN port of the BIPAC 5100S. Turn on your computer and the BIPAC 5100S.
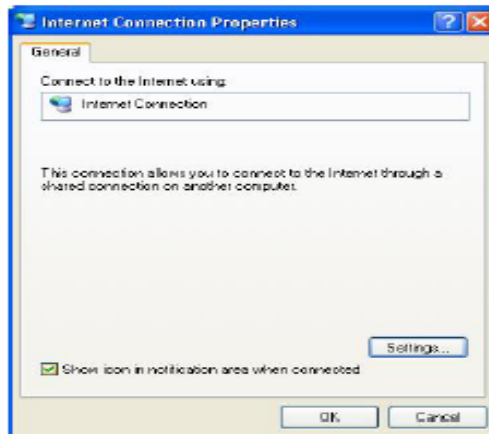
10.4.1 Auto-discover Your UPnP-enabled Network Device

Step 1. Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.
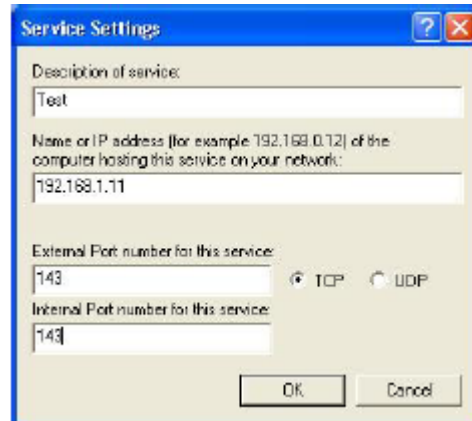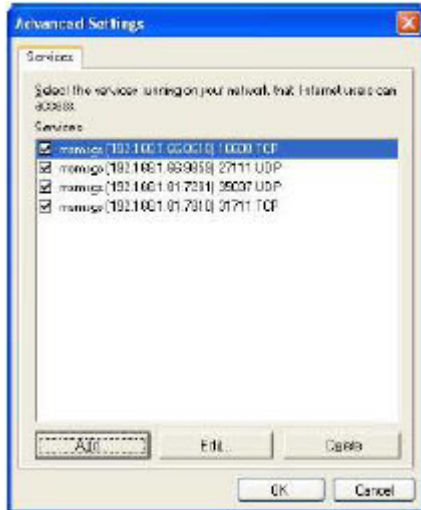
Step 2. Right-click the icon and select Properties.
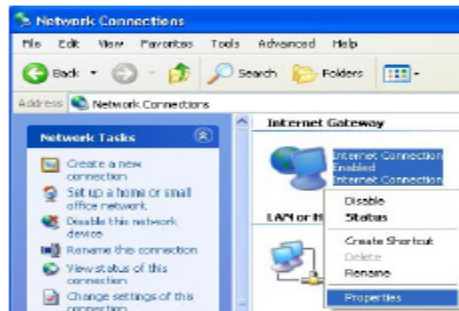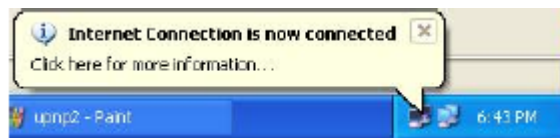

Step 3. In the Internet Connection Properties window, click Settings to see the port mappings there were automatically created.
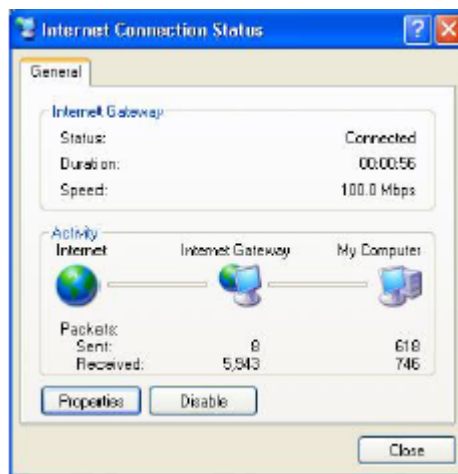

Step 4. You may edit or delete the port mappings or click Add to manually add port mappings.

Step 5. Select Show icon in notification area when connected option and click OK. An icon displays in the system tray

Step 6. Double-click on the icon to display your current Internet connection status.

10.4.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the BIPAC 5100S without finding out the IP address of the BIPAC 5100S first. This comes helpful if you do not know the IP address of the BIPAC 5100S.

Follow the steps below to access the web configurator.

Step 1. Click Start and then Control Panel.

Step 2. Double-click Network Connections.

Step 3. Select My Network Places under Other Places.
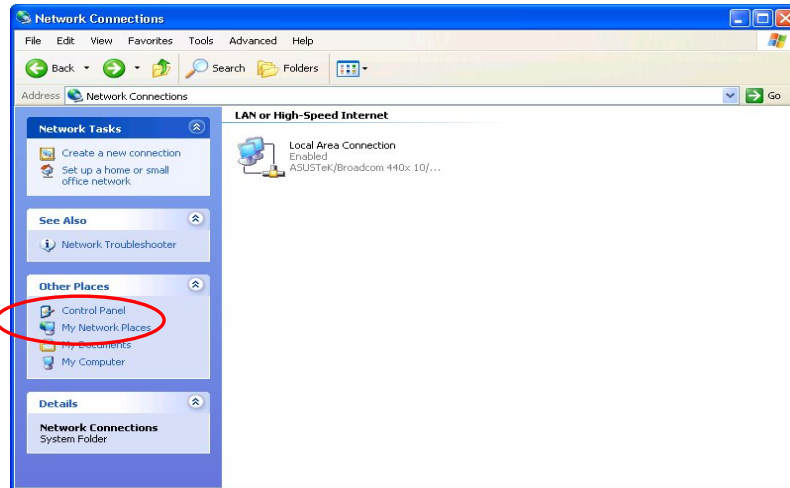
Step 4. An icon with the description for each UPnP-enabled device displays under Local Network.

Step 5. Right-click on the icon for your BIPAC 5100S and select Invoke. The web configurator login screen displays.
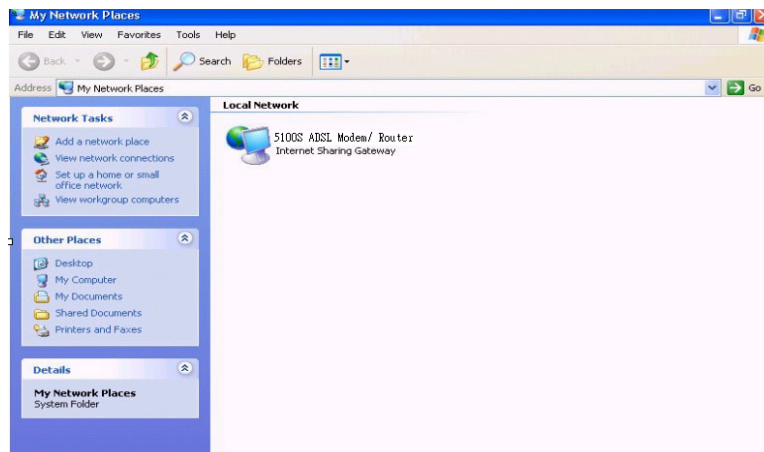
Step 6. Right-click on the icon for your BIPAC 5100S and select Properties. A properties window displays with basic information about the BIPAC 5100S.

Chapter11

Maintenance

This chapter displays system information such as Billion firmware, port IP addresses and port traffic statistics.

11.1 Maintenance Overview

Use the maintenance screens to view system information, upload new firmware, manage configuration and restart your BIPAC 5100S.

11.2 System Status Screen

Click System Status, where you can use to monitor your BIPAC 5100S. Note that these fields are READ-ONLY and are meant to be used for diagnostic purposes.

System Status

System Status

System Name : router
RAS F/W Version: 3.40(TE.2)a10.8.2.20 | 3/23/2004
DSL FW Version: TrendChip, FwVer:2.20.6_A_TC HwVer:T36.F20_1.1
Standard:Multi-Mode

WAN Information:

IP Address:0.0.0.0
IP Subnet Mask:0.0.0.0
Default Gateway:0.0.0.0
VPI/VCI:0/ 32

LAN Information:

MAC Address:00:04:ed:01:23:45
IP Address: 192.168.1.254
IP Subnet Mask: 255.255.255.0
DHCP: Server
DHCP Start IP: 192.168.1.100
DHCP Pool Size: 100

Show Statistics

The following table describes the labels in this screen.

LABEL	DESCRIPTION
System Status	
System Name	This is the name of your BIPAC 5100S. It is for identification purposes.
RAS F/W Version	This is the firmware version and the date created.
DSL FW Version	This is the DSL firmware version associated with your BIPAC 5100S.
Standard	This is the standard that your BIPAC 5100S is using.
WAN Information	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port IP subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in

	the first Wizard screen.
LAN Information	
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your BIPAC 5100S.
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the WAN port DHCP role - **Server**, **Relay** (not all BIPAC 5100S models) or **None**.
DHCP Start IP	This is the first of the contiguous addresses in the IP address pool.
DHCP Pool Size	This is the number of IP addresses in the IP address pool.
Show Statistics	Click **Show Statistics** to see router performance statistics such as number of packets sent and number of packets received for each port.

11.2.1 System Statistics

Click Show Statistics in the System Status screen to open the following screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)".

The Poll Interval(s) field is configurable.
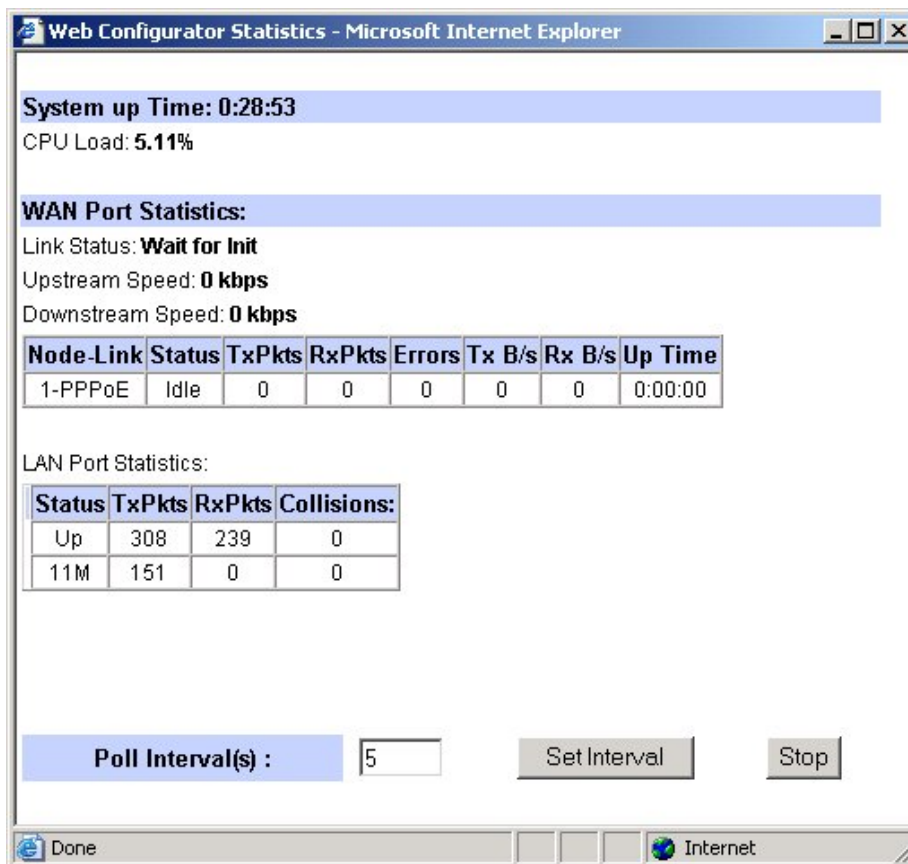
The following table describes the labels in this screen.

LABEL	DESCRIPTION
System up Time	This is the elapsed time the system has been up.

CPU Load	This field specifies the percentage of CPU utilization.
WAN Port Statistics	This is the WAN port.
Link Status	This is the status of your WAN link.
Transfer Rate	This is the transfer rate in kbps.
Upstream Speed	This is the upstream speed of your BIPAC 5100S.
Downstream Speed	This is the downstream speed of your BIPAC 5100S.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
LAN Port Statistics	This is the LAN port.
Interface	This field displays the type of port.
Status	For the WAN port, this displays the port speed and duplex setting if you're using Ethernet encapsulation and **down** (line is down), **idle** (line (ppp) idle), **dial** (starting to trigger a call) and **drop** (dropping a call) if you're using PPPoE encapsulation. For a LAN port, this shows the port speed and duplex setting.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
Collisions	This is the number of collisions on this port.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval** field above.
Stop	Click this button to halt the refreshing of the system statistics.

11.3 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the BIPAC 5100S as a DHCP server or disable it. When configured as a server, the BIPAC 5100S provides the TCP/IP configuration for the clients. If set to None, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.
Click MAINTENANCE, and then the DHCP Table tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including IP Address, Host Name and MAC Address) of all network clients using the DHCP server.

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Host Name	This is the name of the host computer.
IP Address	This field displays the IP address relative to the **Host Name** field.
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed host name. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:AA:BB:00:00:02.

11.4 Diagnostic Screens

These read-only screens display information to help you identify problems with the BIPAC 5100S.

Click Diagnostic to display the following screen.

11.4.1 Diagnostic General Screen

Click Diagnostic and then General to open the screen shown next.

Diagnostic - General

```
- Info -
```

TCP/IP

Address [_____] [Ping]

System

[Reset System]

[Back]

The following table describes the labels in this screen.

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered.
Reset System	Click this button to reboot the BIPAC 5100S. A warning dialog box is then displayed asking you if you're sure you want to reboot the system. Click **OK** to proceed.
Back	Click this button to go back to the main **Diagnostic** screen.

11.4.2 Diagnostic DSL Line Screen

Click Diagnostic and then DSL Line to open the screen shown next.

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
ATM Status	Click this button to view ATM status.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The BIPAC 5100S sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the BIPAC 5100S. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.
Upstream Noise Margin	Click this button to display the upstream noise margin.
Downstream Noise Margin	Click this button to display the downstream noise margin.
Back	Click this button to go back to the main **Diagnostic** screen.

NOTE: DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

11.5 Firmware Screen

Find firmware at www.billion.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "BIPAC 5100S.bin". The upload process uses FTP (File Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. Click Firmware to open the following screen. Follow the instructions in this screen to upload firmware to your BIPAC 5100S.

FIRMWARE

Firmware Upgrade

To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click UPLOAD.

File Path: [   ] [Browse...] [Upload]

CONFIGURATION FILE

Click Reset to clear all user-defined configurations and return to the factory defaults.

[Reset]

The following table describes the labels in this screen.

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.
Reset	Click this button to clear all user-entered configuration information and return the BIPAC 5100S to its factory defaults. Refer to the Resetting the BIPAC 5100S section.

After you see the Firmware Upload in Process screen, wait two minutes before logging into the BIPAC 5100S again.

The BIPAC 5100S automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.
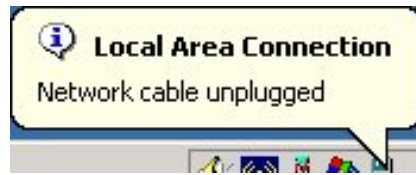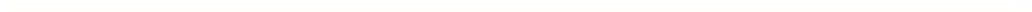

After two minutes, log in again and check your new firmware version in the System Status screen.

If the upload was not successful, the following screen will appear. Click Back to go back to the Firmware screen.

Appendix
Troubleshooting

This chapter covers potential problems and the corresponding remedies.

A.1 Using LEDs to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

A.1.1 Power LED

The PWR LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Make sure that the BIPAC 5100S's power adaptor is connected to the BIPAC 5100S and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the BIPAC 5100S and the power source are both turned on and the BIPAC 5100S is receiving sufficient power.
3	Turn the BIPAC 5100S off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

A.1.2 LAN LED

The LAN LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Check the Ethernet cable connections between your BIPAC 5100S and the computer or hub.
2	Check for faulty Ethernet cables.
3	Make sure your computer's Ethernet card is working properly.
4	If these steps fail to correct the problem, contact your local distributor for assistance.

A.1.3 DSL LED

The DSL LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Check the telephone wire and connections between the BIPAC 5100S DSL port and the wall jack.
2	Make sure that the telephone company has checked your phone line and set it up for DSL service.

3	Reset your ADSL line to reinitialize your link to the DSLAM. For details, refer to the *Maintenance* chapter (web configurator) or the System Information and Diagnosis chapter.
4	If these steps fail to correct the problem, contact your local distributor for assistance.

A.2 Telnet

I cannot telnet into the BIPAC 5100S.

STEPS	CORRECTIVE ACTION
1	Check the LAN port and the other Ethernet connections.
2	Make sure you are using the correct IP address of the BIPAC 5100S. Check the IP address of the BIPAC 5100S.
3	Ping the BIPAC 5100S from your computer. If you cannot ping the BIPAC 5100S, check the IP addresses of the BIPAC 5100S and your computer. Make sure your computer is set to get a dynamic IP address; or if you want to use a static IP address on your computer, make sure that it is on the same subnet as the BIPAC 5100S.
4	Make sure you entered the correct password. The default password is "admin". If you have forgot your username or password, refer to *Section A.5*.
5	If these steps fail to correct the problem, contact the distributor.

A.3 Web Configurator

I cannot access the web configurator.

STEPS	CORRECTIVE ACTION
1	Make sure you are using the correct IP address of the BIPAC 5100S. Check the IP address of the BIPAC 5100S.
2	Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details.
3	For WAN access, you must configure remote management to allow server access from the Wan (or all).
4	Your computer's and the BIPAC 5100S's IP addresses must be on the same subnet for LAN access.
5	If you changed the BIPAC 5100S's LAN IP address, then enter the new one as the URL.
6	Remove any filters in LAN or WAN that block web service.
7	See also *Section A.9*.

The web configurator does not display properly.

STEPS	CORRECTIVE ACTION
1	Make sure you are using Internet Explorer 5.0 and later versions.
2	Delete the temporary web files and log in again. In Internet Explorer, click **Tools**, **Internet Options** and then click the **Delete Files ...** button. When a **Delete Files** window displays, select **Delete all offline content** and click **OK**. (Steps may vary depending on the version of your Internet browser.)

A.4 Login Username and Password

I forgot my login username and/or password.

STEPS	CORRECTIVE ACTION
1	If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This will erase all custom configurations and restore all of the factory defaults including the password.
2	Press the **RESET** button for five seconds, and then release it. When the **SYS** LED begins to blink, the defaults have been restored and the BIPAC 5100S restarts.
3	The default username is "admin". The default password is "admin". The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing.
4	It is highly recommended to change the default username and password. Make sure you store the username and password in a save place.

A.5 LAN Interface

I cannot access the BIPAC 5100S from the LAN or ping any computer on the LAN.

STEPS	CORRECTIVE ACTION
1	Check the Ethernet LED on the front panel. A LAN LED should be on if the port is connected to a computer or hub. If the 10M/100M LED on the front panel are both off, refer to *Section A.1.2*.
2	Make sure that the IP address and the subnet mask of the BIPAC 5100S and your computer(s) are on the same subnet.

A.6 WAN Interface

Initialization of the ADSL connection failed.

STEPS	CORRECTIVE ACTION
1	Check the cable connections between the ADSL port and the wall jack. The DSL LED

	on the front panel of the BIPAC 5100S should be on.
2	Check that your VPI, VCI, type of encapsulation and type of multiplexing settings are the same as what you collected from your telephone company and ISP.
3	Restart the BIPAC 5100S. If you still have problems, you may need to verify your VPI, VCI, type of encapsulation and type of multiplexing settings with the telephone company and ISP.

I cannot get a WAN IP address from the ISP.

STEPS	CORRECTIVE ACTION
1	The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name.
2	The username and password apply to PPPoE and PPoA encapsulation only. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (be sure to use the correct casing).

A.7 Internet Access

I cannot access the Internet.

STEPS	CORRECTIVE ACTION
1	Make sure the BIPAC 5100S is turned on and connected to the network.
2	If the DSL LED is off, refer to *Section A.1.3*.
3	Verify your WAN settings.
4	Make sure you entered the correct user name and password.
5	For wireless stations, check that both the BIPAC 5100S and wireless station(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated).

Internet connection disconnects.

STEPS	CORRECTIVE ACTION
1	Check the schedule rules.
2	If you use PPPoA or PPPoE encapsulation, check the idle time-out setting.
3	Contact your ISP.

A.8 Remote Management

I cannot remotely manage the BIPAC 5100S from the LAN or WAN.

STEPS	CORRECTIVE ACTION
1	Refer to the Remote Management Limitations section in the Firmware and Configuration File Management chapter for scenarios when remote management may not be possible.
2	Use the BIPAC 5100S's WAN IP address when configuring from the WAN. Use the BIPAC 5100S's LAN IP address when configuring from the LAN.

3	Refer to Section A.6 for instructions on checking your LAN connection.
	Refer to Section A.7 for instructions on checking your WAN connection.
4	See also the Section A.4.

A.9 Remote Node Connection

I cannot connect to a remote node or ISP.

STEPS	CORRECTIVE ACTION
1	Check WAN screen to verify that the username and password are entered properly.
2	Verify your login name and password for the remote node.
3	If these steps fail, you may need to verify your login and password with your ISP.

Product Support and Contact Information

Most problems can be solved by referring to the **Troubleshooting** section in the User's Manual. If you cannot resolve the problem with the **Troubleshooting** chapter, please contact the dealer where you purchased this product.

Contact Billion

AUSTRALIA

http://www.billion.com.au

©2004 Billion Electric Co., Ltd. PC Range P/L. All Rights Reserved.

WORLDWIDE

http://www.billion.com